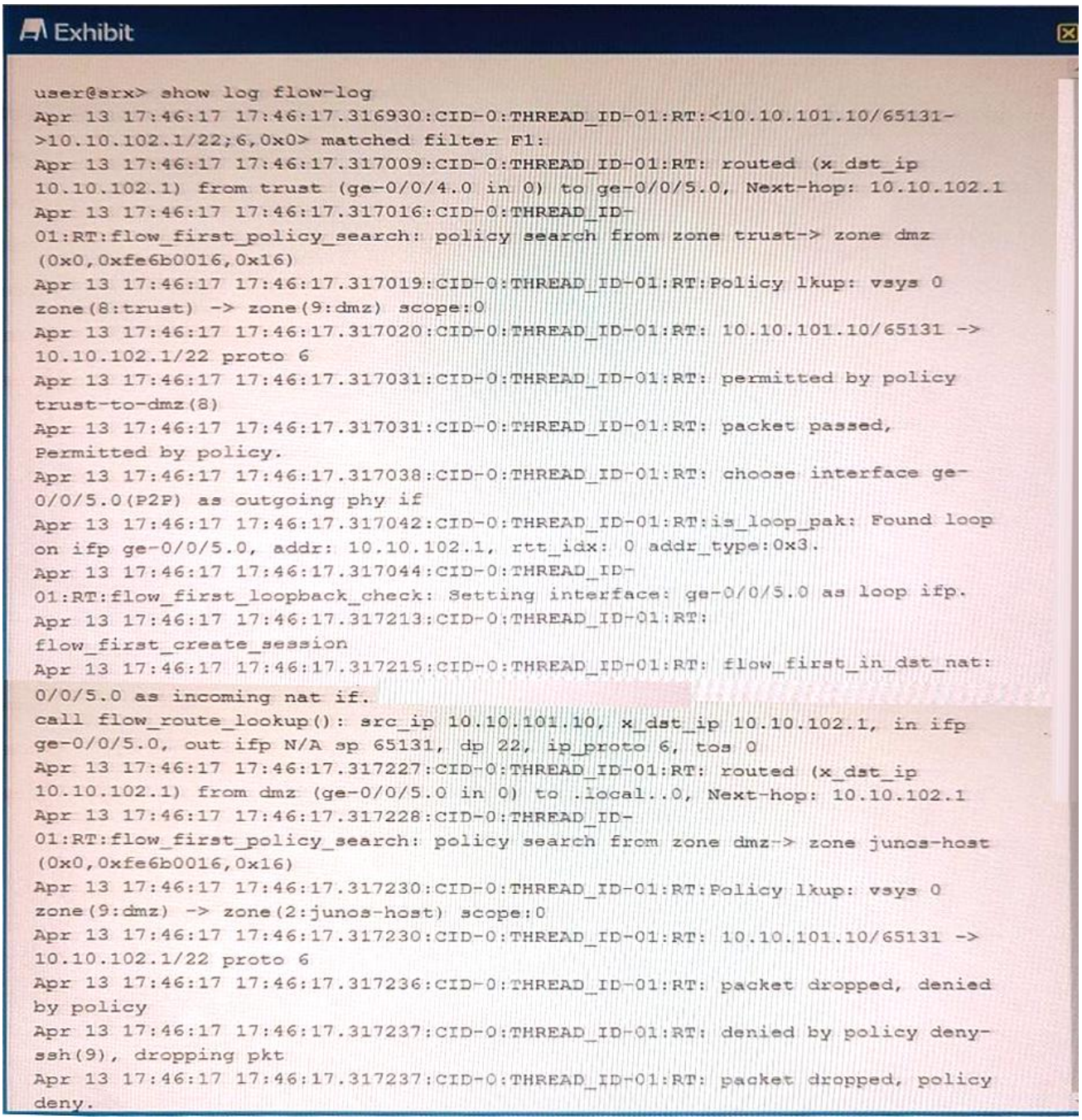
Exam : **JN0-636**

Title : Security,Professional (JNCIP-SEC)

https://www.passcert.com/JN0-636.html

1.Exhibit



You are using traceoptions to verify NAT session information on your SRX Series device. Referring to the exhibit, which two statements are correct? (Choose two.)

A. This is the last packet in the session.

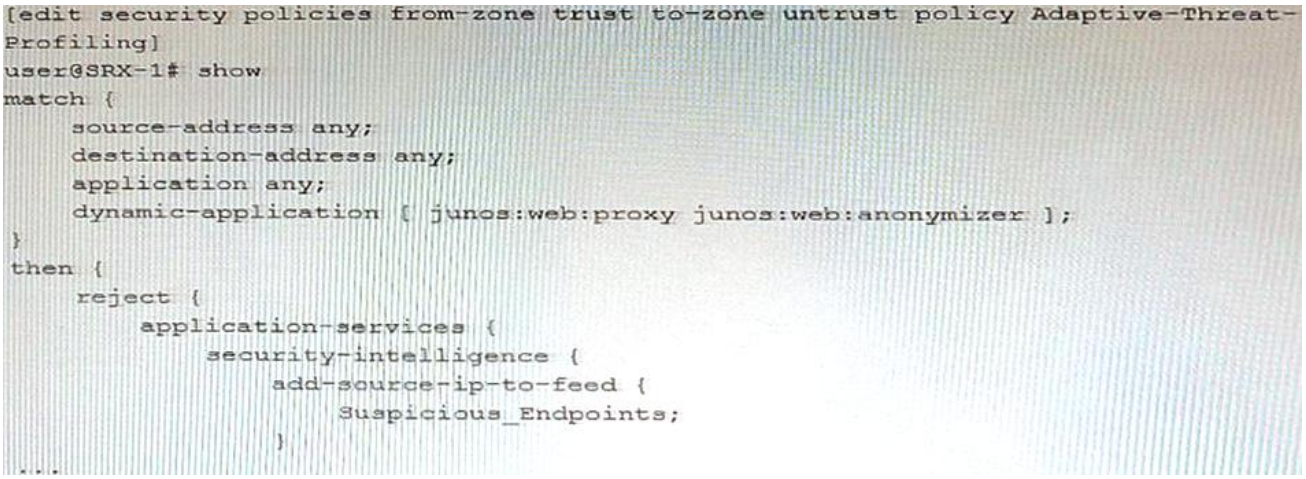
B. The SRX Series device is performing both source and destination NAT on this session.

C. This is the first packet in the session.

D. The SRX Series device is performing only source NAT on this session.

Answer: A,B

2.Exhibit



Referring to the exhibit, which two statements are true? (Choose two.)

A. The 3uspicious_Endpoint3 feed is only usable by the SRX-1 device.

B. You must manually create the suspicious_Endpoint3 feed in the Juniper ATP Cloud interface.

C. The 3uspiciou3_Endpoint3 feed is usable by any SRX Series device that is a part of the same realm as SRX-1

D. Juniper ATP Cloud automatically creates the 3uopi'cioua_Endpoints feed after you commit the security policy.

Answer: A,C

3.You are required to deploy a security policy on an SRX Series device that blocks all known Tor network IP addresses.

Which two steps will fulfill this requirement? (Choose two.)

A. Enroll the devices with Juniper ATP Appliance.

B. Enroll the devices with Juniper ATP Cloud.

C. Enable a third-party Tor feed.

D. Create a custom feed containing all current known MAC addresses.

Answer: A,D

4.You are not able to activate the SSH honeypot on the all-in-one Juniper ATP appliance.

What would be a cause of this problem?

A. The collector must have a minimum of two interfaces.

B. The collector must have a minimum of three interfaces.

C. The collector must have a minimum of five interfaces.

D. The collector must have a minimum of four interfaces.

Answer: D

Explanation:

https://www.juniper.net/documentation/en_US/release-independent/jatp/topics/task/configuration/jatp-traffic-collectorsetting-ssh-honeypot-detection.html

5.Exhibit

```
[edit security ike gateway advpn-gateway]
user@srx# show
ike-policy advpn-policy;
address 192.168.3.1;
local-identity distinguished-name;
remote-identity distinguished-name container O=Juniper;
external-interface ge-0/0/3.0;
version v2-only;
[edit interfaces]
user@srx# show st0
unit 0 {
    family inet {
        address 10.100.100.1/24;
    }
}
```

Referring to the exhibit, a spoke member of an ADVPN is not functioning correctly.
Which two commands will solve this problem? (Choose two.)
A)

```
[edit interfaces]
user@srx# set st0.0 multipoint
```

B)

```
[edit security ike gateway advpn-gateway]
user@srx# set advpn suggester disable
```

C)

```
[edit security ike gateway advpn-gateway]
user@srx# set local-identity inet advpn
```

D)

```
[edit security ike gateway advpn-gateway]
user@srx# set advpn partner disable
```

A. Option A
B. Option B
C. Option C
D. Option D
Answer: C

6.You are asked to download and install the IPS signature database to a device operating in chassis cluster mode.
Which statement is correct in this scenario?
A. You must download and install the IPS signature package on the primary node.
B. The first synchronization of the backup node and the primary node must be performed manually.
C. The first time you synchronize the IPS signature package from the primary node to the backup node, the primary node must be rebooted.
D. The IPS signature package must be downloaded and installed on the primary and backup nodes.
Answer: D

7.Which two additional configuration actions are necessary for the third-party feed shown in the exhibit to work properly? (Choose two.)
A. You must create a dynamic address entry with the IP filter category and the ipfilter_office365 value.
B. You must create a dynamic address entry with the C&C category and the cc_offic365 value.
C. You must apply the dynamic address entry in a security policy.
D. You must apply the dynamic address entry in a security intelligence policy.
Answer: A,C

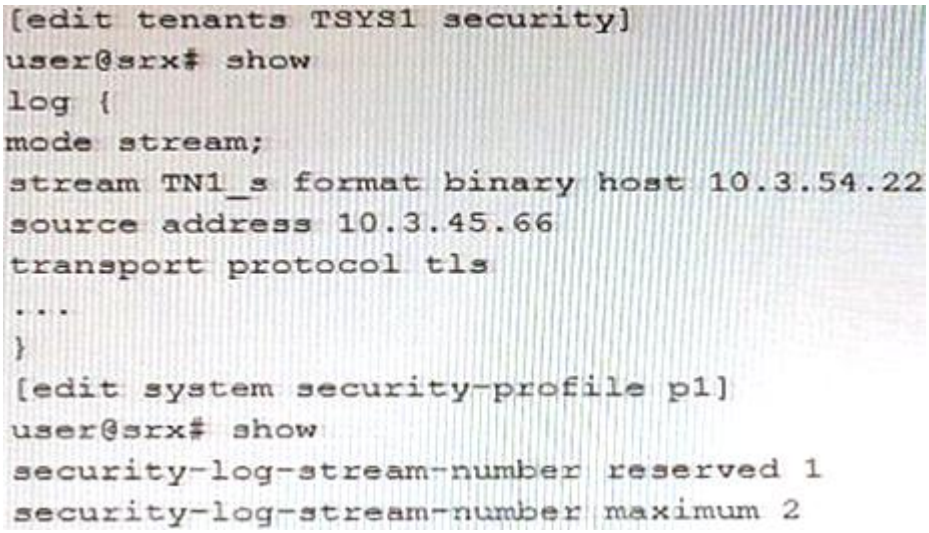
8.Exhibit

```
user@SRX> show security flow session
...
Session ID: 4546, Policy name: policy1/8, Timeout: 4, Valid
  In: 10.10.10.2/6 --> 10.10.20.2/1382;icmp, Conn Tag 0x0, If: st0.0, Pkts: 1,
Bytes: 84
  Out: 10.20.20.2/1382 --> 10.10.10.2/6;icmp, Conn Tag 0x0, If: ge-0/0/3.0,
Pkts: 1, Bytes: 84
Session ID: 4547, Policy name: policy2/9, Timeout: 4, Valid
  In: 10.20.20.2/226 --> 10.10.10.2/38703;icmp, Conn Tag 0x0, If: ge-0/0/3.0,
Pkts: 1, Bytes: 84
  Out: 10.10.10.2/38703 --> 10.10.20.2/226;icmp, Conn Tag 0x0, If: st0.0, Pkts:
1, Bytes: 84
Total sessions: 13
```

You are validating bidirectional traffic flows through your IPsec tunnel. The 4546 session represents traffic being sourced from the remote end of the IPsec tunnel. The 4547 session represents traffic that is sourced from the local network destined to the remote network.
Which statement is correct regarding the output shown in the exhibit?
A. The remote gateway address for the IPsec tunnel is 10.20.20.2
B. The session information indicates that the IPsec tunnel has not been established
C. The local gateway address for the IPsec tunnel is 10.20.20.2
D. NAT is being used to change the source address of outgoing packets
Answer: A

9.What is the purpose of the Switch Microservice of Policy Enforcer?
A. to isolate infected hosts
B. to enroll SRX Series devices with Juniper ATP Cloud
C. to inspect traffic for malware
D. to synchronize security policies to SRX Series devices
Answer: B

10.Exhibit



```
[edit tenants TSYS1 security]
user@srx# show
log {
mode stream;
stream TN1_s format binary host 10.3.54.22
source address 10.3.45.66
transport protocol tls
...
}
[edit system security-profile p1]
user@srx# show
security-log-stream-number reserved 1
security-log-stream-number maximum 2
```

An administrator wants to configure an SRX Series device to log binary security events for tenant systems.

Referring to the exhibit, which statement would complete the configuration?

A. Configure the tenant as TSYS1 for the pi security profile.

B. Configure the tenant as root for the pi security profile.

C. Configure the tenant as master for the pi security profile.

D. Configure the tenant as local for the pi security profile

Answer: B